Runecast

CNAPP
BUYER'S GUIDE 2023

A comprehensive guide on selecting the best Cloud Native Application Protection Platform for your organization

High Performer WINTER 2023

Best Support WINTER 2023

Gartner COOL VENDOR 2020

www.runecast.com

Table of Contents

The Emergence of Cloud Native Application Protection Platforms (CNAPPs) 03
The need for faster release cycles 03
The need for a consolidated security solution to grasp technology complexity 03
The skyrocketing business costs of security incidents 04
The cost of multiple solutions within your environment 04

Key Benefits of CNAPPs for an Organization's Ability to Deliver Faster 05

Core Components of Integrated CNAPPs Every Business and IT Leader Should Understand 06
Cloud Workload Protection Platform (CWPP) 06
Cloud Security Posture Management (CSPM) 07
Cloud Infrastructure Entitlement Management (CIEM) 08
CI/CD Security and Container scanning 08

Evaluating and Choosing the Best-Fit CNAPP Solution 09

Conclusion 10

The Emergence of Cloud Native Application Protection Platforms (CNAPPs)

Cloud technology has been a milestone in transforming business and IT forever, bringing many benefits and no shortage of major challenges. Since 2020, there has been a **50% increase** in cloud usage. Gartner has stated that more than **85% of organizations** will embrace a cloud-first principle by 2025 and will not be able to fully execute on their digital strategies without the use of cloud-native architectures and technologies (Gartner, 2021).

While modern enterprises migrate to the cloud as needed, it often ends up with a heterogeneous mix of fragmented security products managed by siloed security teams and a plethora of unanswered complexity and security questions.

Recent market and industry developments have imposed new challenges for which modern organizations struggle to find answers. These challenges can be summarized as follows:

1. THE NEED FOR FASTER RELEASE CYCLES

According to the Cloud Native Computing Foundation (CNCF) Survey, **55%** of respondents release code weekly or more frequently and **18%** of respondents release code multiple times per day. Additionally, **53%** of respondents check in code multiple times per day (CNCF Survey, 2020). With daily and weekly releases, a traditional application security approach that gates releases before going into production for security testing nullifies the speed and agility of digital transformation. As a result, organizations strive to find and resolve application vulnerabilities early in the development cycle, rather than paying the price in production.

2. THE NEED FOR A CONSOLIDATED SECURITY SOLUTION TO GRASP TECHNOLOGY COMPLEXITY

As both applications and infrastructure grow more diverse and distributed along with organizations' scale, the requirements to resolve security complexity is rising. Modern enterprises struggle to respond to the need for broader security workflows that can address different security issues – including vulnerability management and compliance – across various platforms and applications.

More than **80%** of companies are already deploying across hybrid and multi cloud (Thomson Reuters, 2021). With more technologies to manage, the more problems security and business leaders are likely to face. This stretches security professionals and their resources. CISOs struggle to staff and train their teams as they take on more tools. It is unsustainable as constantly reviewing dashboards, alerts and data has proven to lead to burnout, organizational risk and, in many cases, huge associated costs.

Around **64% of IT professionals** report that the complexity of their organization's IT infrastructure slows IT operations and digital initiatives (ESG Global, 2021).

3. THE SKYROCKETING BUSINESS COSTS OF SECURITY INCIDENTS

According to a recent IBM report, the average data breach costs businesses in the United States **$9.05 million**. The Log4j zero day vulnerability affected (and continues to affect) hundreds of millions of apps and devices, and the costs of data violation reached **$888 million** (IBM, Costs of Data Breach, 2022). The costs of neglecting security and compliance continue to rise, making it paramount for organizations to leverage the sustainable solution that allows for finding and resolving vulnerabilities early in the software development process.

4. THE COST OF MULTIPLE SOLUTIONS WITHIN YOUR ENVIRONMENT

Within many organizations, DevOps and DevSecOps teams are using different solutions to achieve the same goal due to team-based budgeting. Purchasing decisions are made separately by each team without consideration for consolidation of monitoring tools to achieve a global outcome. This siloed approach not only costs the company money for multiple solutions which achieve the same end goal, but also removes any possibility of global visualization within environments and hinders team collaboration.

Around **63% of IT professionals** state that the lack of visibility into spending specifics for public cloud hinders IT planning (ESG Global, 2021).

Where SecOps teams require DevOps teams to implement company-specific security governance, they have no visibility into what the DevOps team has implemented, which in turn incurs time costs for report sharing. Without a solution to create a custom company security framework, many teams become reliant on spreadsheets, to address internal policy reporting which again costs time. This is also inefficient where customized templates within a solution could be used to track internal policies and provide reporting.

Cloud-Native Application Protection Platforms (CNAPPs) address these challenges and provide business and IT leaders with a consolidated solution that streamlines DevOps and SecOps efforts, allowing the teams to work jointly in achieving ambitious development goals, securely.

The term was coined by Gartner in 2021 and is defined as:

> *"an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production. CNAPPs consolidate a large number of previously siloed capabilities, including container scanning, cloud security posture management, infrastructure as code scanning, cloud infrastructure entitlements management and runtime cloud workload protection platforms."*

Cloud-native application protection platforms (CNAPPs) enable organizations to leapfrog the cost and complexity of siloed security products to have instead a continuous security fabric without major investments in multiple tools or developer talent.

PROTIP

Evaluate industry changes and trends through the prism of your development lifecycle. How do they impact your ability to deliver modern application development quickly and securely?

Key Benefits of CNAPPs for an Organization's Ability to Deliver Faster

CNAPP provides many benefits to organizations by not only consolidating visualization of all technology issues into one platform, but also alleviating the time taken to utilize multiple tools, to therefore create a proactive environment within organizations teams. Being able to proactively visualize issues across hybrid and multi cloud infrastructure, enables DevOps and DevSecOps teams to quickly see and remediate issues before they can put you at greater risk, ensuring secure environments with maximum uptime, which in turn reduces company costs.

Among other key benefits of CNAPP adoption are:

- Closing the gaps in visibility and optimizing the observability across configurations, assets, permissions, code, and workloads
- Integrating security scanning capabilities into the development pipeline
- Automating processes for remediation that take place as early in the software lifecycle as possible, consequently organizations see the reduction of costs and operational complexity
- Security at the speed of DevOps allows for more secure application building, with more efficiency and less burden – the earlier security issues are flagged, the sooner developers can identify and fix critical bugs and vulnerabilities before they release software to production environments, therefore minimizing the risk of data breaches, downtime or an infrastructure exposure to attacks
- Guardrails help distribute 'security' responsibility, meaning enabling developers to be in control of security at each level of the development cycle, reducing the friction between Security, DevOps and ITOM teams

PROTIP

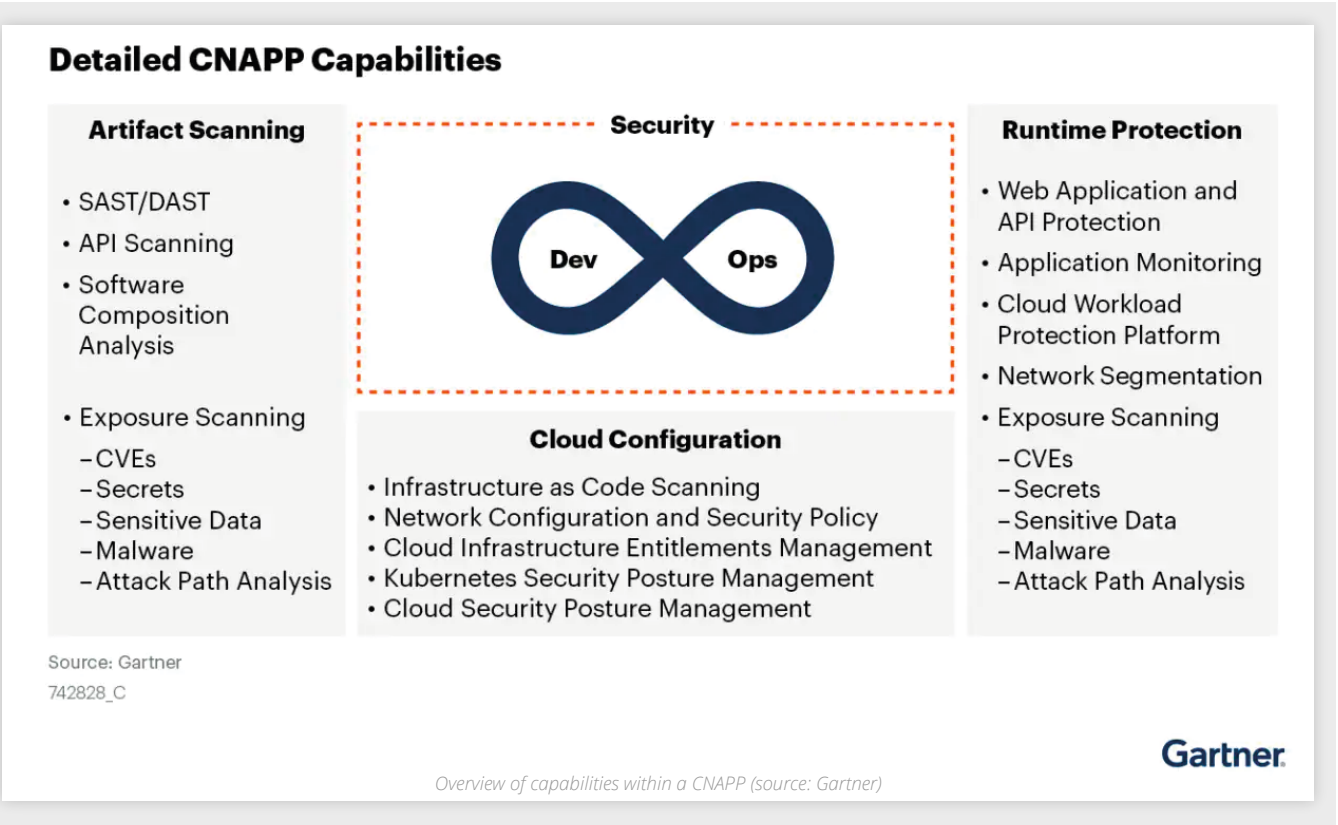
The best-fit CNAPP solution is the one that meets the specific business needs of your organization. Define use cases and understand how you will measure success. Get answers to such questions as why you need a CNAPP, which KPIs are important for you and what ROI you are anticipating.

Core Components of Integrated CNAPPs Every Business and IT Leader Should Understand

An effective CNAPP helps security teams by providing them with a single view into the organization's biggest risks, so that they can tackle and optimize security and compliance early in the development stage of application lifecycle – and minimize friction.

When looking at CNAPP solutions, it is crucial to know the most essential components that every business and tech leader should understand. Among the fundamental capabilities of a proper cloud-native application protection platform are:

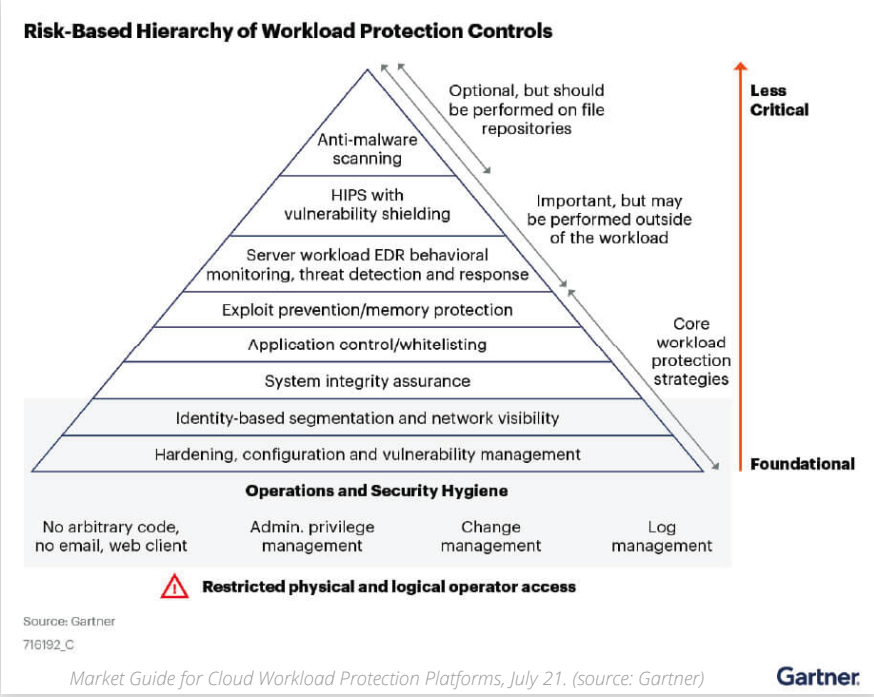
1. Cloud Workload Protection Platform (CWPP)
2. Cloud Security Posture Management (CSPM)
3. Cloud Infrastructure Entitlement Management (CIEM)
4. CI/CD Security and Container scanning



Overview of capabilities within a CNAPP (source: Gartner)

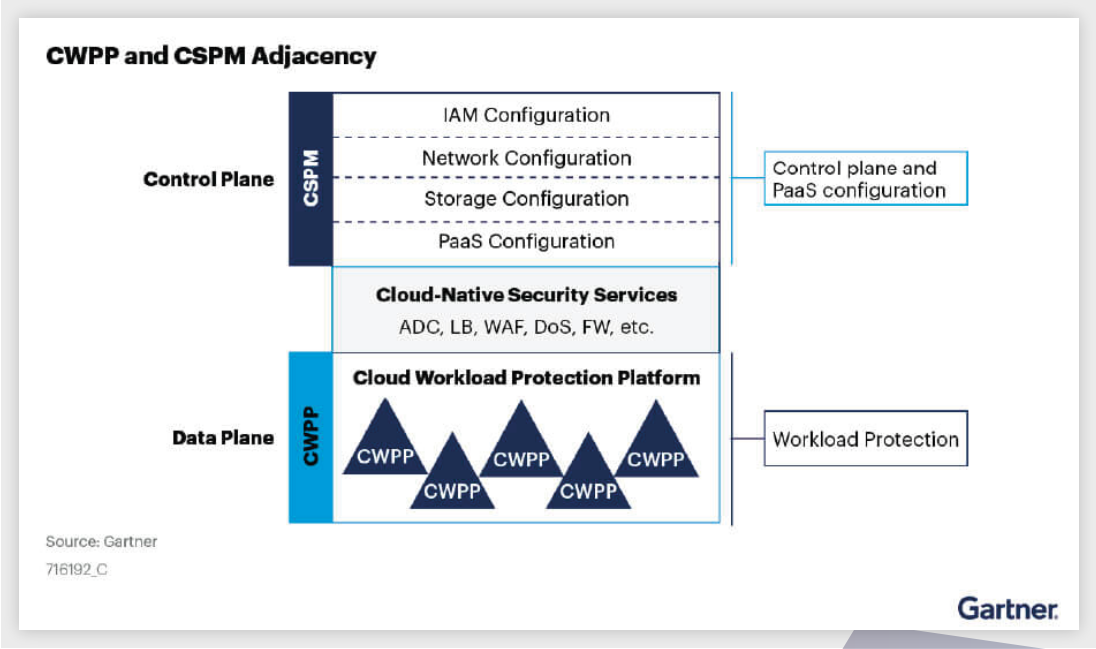
1. **Cloud Workload Protection Platform (CWPP)** is a category for a software solution that secures cloud-based workloads. What that means, in practice, is one piece of software that will protect your cloud environments. One dashboard or interface to view, the so-called 'single source of truth' that shows not just one environment but all your environments. This reduces time spent checking dashboards for security professionals and the possibility of missing a potentially critical alert. Features of a CWPP can include intrusion prevention and malware scanning but are specifically catered to the cloud.

CWPP solutions are built for security in the cloud era and should cover on-premises, physical and virtual machines, containers, or basically all the ingredients of the modern hybrid and multi cloud environment.



Market Guide for Cloud Workload Protection Platforms, July 21. (source: Gartner)

2. **Cloud Security Posture Management (CSPM)** is a way of protecting workloads from threats due to misconfigurations. Many organizations rely on public cloud infrastructure but don't know the best practice or best configuration of that cloud. When the cloud provider you are reliant on changes or adds a new feature, you need to know how to handle the effects that might have on your existing configurations. CSPM is the practice of monitoring infrastructure, detecting misconfiguration throughout the environment and resolving it using best practices and documented fixes. Good CSPM tools use multiple sources of information to automate the finding of the best and most secure setup for your needs.



3. The main goal of **Cloud Infrastructure Entitlement Management (CIEM)** solution is to manage identities and their end-to-end entitlements. CIEM solutions will inventory all identities, person and non-person, and reveal all effective permissions, illuminating potential attack paths. This allows your business to strip excessive permissions and work towards policies like least privilege. CIEM solutions will keep you at 'least privileged' with continuous monitoring to notify you of any out-of-policy changes.

4. **CI/CD security together with container scanning** facilitates secure releases of cloud applications. According to the CNCF Survey, **82% of respondents** use CI/CD pipelines in production as well as the use of containers in production has **increased to 92%**.

   As containers are primarily the building blocks of cloud native applications, organizations need a simple and secure way to manage them. Without the right solution to check containers in the development stage, DevOps and DevSecOps teams struggle to ensure that containers released into production are secure.

   Even though Kubernetes is a separate platform on its own, it automates container operations and ensures errorless deployment and scale of containerized applications. Not a surprise that Kubernetes use in production has **increased to 83%** (CNCF Survey, 2020).

   According to "The State of Kubernetes" survey, almost half (48%) of respondents expect the number of **Kubernetes clusters** they operate **to grow by more than 50%**; an additional 28% expect the number of clusters to increase notably (20% to 50%) in the coming year (VMware, 2022).

   Thus, a Cloud Native Application Protection Platform (CNAPP) enabling CISOs, CIOs, DevOps and DevSecOps teams with proactive Kubernetes Security Posture Management, provides visibility of cluster misconfigurations, security vulnerabilities and potential issues in their workloads.

   It is paramount to be able to scan containers for vulnerabilities and compliance early in the development stage. This need assembled in the DevOps development pipeline catalyzes the **shift-left approach** of moving security checks sooner in the development cycle. This shift allows the execution of security testing and best practices along the entire development cycle, detecting and remediating potential security issues and vulnerabilities before moving to production. This approach is easier, more cost-effective and boosts DevOps and DevSecOps teams performance.

PROTIP

Focus on the key capabilities and features of a CNAPP that fits best to your security strategy and meets your specific objectives. The most sophisticated CNAPP with outstanding capabilities and all the bells and whistles might not answer your business needs and therefore will be a waste of money.

Evaluating and Choosing the Best-Fit CNAPP Solution

Before fully committing to investing a particular CNAPP solution, it's recommended to review the demo or have a call with a solution engineer who will guide you through the full set of features and capabilities. This will help you to understand the difference between pre-set demos and the full capabilities of the system you are evaluating. Having a good understanding of how the capabilities answer your business needs (functionality and strategy-fit) is paramount. Also, request a full scope of the project and the implementation objectives. This will give you a clear understanding of whether the solution addresses your initial strategy.

KEY QUESTIONS TO ASK BEFORE CHOOSING A CLOUD NATIVE APPLICATION PROTECTION PLATFORM:

1. Which technologies do you need to protect in your organisation?
2. Does the solution enable full visibility for team collaboration?
3. Does the solution provide reporting on a team basis and globally?
4. Which key components does it offer (i.e. CWPP, CSPM, KSPM, etc) that fit your organization's needs?
5. Is this a single platform or a consolidation of different products priced separately?
6. How does the solution ensure integrated security across our entire application lifecycle?
7. How will it integrate into your development cycles?
8. Does the solution provide monitoring for other technologies deployed in your (AWS, Azure or GCP) cloud environment, such VMware, Kubernetes, and Operating Systems (OS)?
9. Kubernetes is a widely used platform by enterprises to manage and scale containers in a cloud environment. Does the vendor support Kubernetes Security Posture Management (KSPM)?
10. Does it fulfill the needs of the DevOps CI/CD pipeline providing the shift-left approach?
11. Does it provide runtime security monitoring once the containers are deployed?
12. What deployment options are available to suit your environment, on premises and/or cloud?
13. Does the platform have the ability to run in air-gapped sites? (Notable for government, military and financial institutions)

PROTIP

The modern security solutions landscape is rapidly changing. That's why the CNAPP solution that you select has to be scalable and flexible enough to grow with your business while adjusting the evolving business needs, objectives and requirements.

Conclusion

Increasingly dynamic environments, the need for faster release cycles, and a growing number of technologies deployed in the cloud all lead to new challenges for cloud security.

Cloud Native Application Protection Platforms emerged as an integrated and consolidated solution for more effective collaboration between Security and DevOps teams, enabling the teams to build, deploy and run secure cloud applications. Therefore, it is crucial to choose the right solution that consolidates all the building blocks together and enables fast and secure development of business applications today and in the future.

When choosing a CNAPP solution, ensure you have taken into account all of your team's needs, by meeting with all team management and supervisors at once. Find out what the global needs are, how the teams are communicating, which areas teams need to share information about, how many disparate tools are being used in the company and therefore how you can consolidate all tools into one platform and save team finances to be used more proactively in other areas.

An integrated CNAPP solution enables DevOps and SecOps teams to work jointly meeting the business objectives, lessens costs and provides a single point of view from production to runtime.

Runecast Solutions Ltd. is a leading global provider of an AI-powered solution for secure and compliant workloads in hybrid and multi cloud environments.

Runecast platform is designed following the CNAPP approach bringing organizations a single source of truth for configuration monitoring, vulnerability management, security, compliance remediation, reporting, and upgrade planning across multiple infrastructure environments. It reduces operational overheads, increases clarity, and efficiently assesses infrastructure vulnerabilities while managing regulatory compliance.

Forward-focused enterprises like Avast, DocuSign, and the German Aerospace Center (DLR) use Runecast.

Headquartered in London, U.K., Runecast is a Gartner Cool Vendor and has won *Computing* awards for **Cloud Security Product of the Year** and **Best Place to Work in Digital**.

Runecast Platform

A Single AI-Powered Platform for Secure and Compliant Workloads Anywhere

Security & Compliance

TEAMS

DevSecOps | SecOps | Compliance

Gain complete visibility, stay fully compliant with a list of standards and ensure continuous remediation for your environment with a single AI-powered platform.

CAPABILITITES

- Cloud Security Posture Management
- Governance, Risk management & Compliance
- Vulnerability Management
- Compliance Tracking

Container Security

TEAMS

Dev | DevSecOps

Secure containerized apps from development to production in minutes. Eliminate any vulnerabilities and policy risks in pre-production to run secure and compliant apps.

CAPABILITITES

- Container Image Scanning
- Kubernetes Security Posture Management
- Kubernetes Admission Controller Integrations
- CI/CD Integrations

Proactive ITOM

TEAMS

IT | DevSecOps

Modernize and make your IT Ops cost-effective by automating vulnerability and best practices scanning of your infrastructure to maintain IT operations health.

CAPABILITITES

- Configuration Drift Management
- Proactive Issue Prevention
- Best Practices Adherence
- Remediation & Reporting

TRY IT FREE